IBM Security Thought Leadership White Paper

Deploy silent security to protect identities and future-proof your IAM

The best identity and access management solution is the one you don’t know is there

IBM Security

Need strong security? Go silent.

A strong security posture and a positive digital experience don't have to be mutually exclusive. You can achieve both with the silent, nonintrusive security of IBM identity and access management (IAM). This approach to IAM isn't hidden away—far from it. Silent security connects users, applications, and ultimately people to the information and applications they need—only standing in the way when it detects bad actors.

Providing users access to the right applications and tools, at the right time, and for the right purposes must be done while offering customers a delightful experience. You need to make sure you are protecting information from theft and meeting ever-stricter regulatory requirements. Your IAM solution is integral to achieving these goals, yet it works best when your users don't even know it's there.

Making access easy means keeping quiet

IBM has been a leader in providing IAM solutions for decades, offering seamless access to millions of employees and consumers. Chances are you've securely accessed consumer services or the applications you need to do your job with IAM technology from IBM. Whether or not you knew it, we've been in the background, quietly validating your access, ensuring you are who you say you are and that your credentials have not been compromised.

That's the way IBM IAM operates—with unobtrusive identity assurance backed by behavioral analytics and risk-based algorithms, minimizing frustration to users, and intervening only when something is wrong. With analytics, you have visibility into your internal and external users and their access to help establish trust across your organization. You can reduce your vulnerable attack surface by ensuring that only the right people have access to sensitive information.

While nearly all users have good intentions, accounts can still be compromised and identities stolen by bad actors. That's when IBM IAM steps in, with sophisticated multi-factor authentication options to verify identity or automatically shut down bad actors in an instant.

A recent IBM study on a top-25 global bank found that fewer than

1%

of its users exhibited rogue behavior.[1]

Read what the experts are saying about good password practices.

1 IBM® Trusteer® research.

Give the right access to the right people

Keeping your business secure from both external attacks and insider threats is at the top of every security leader's mind. You can't ignore either risk: attacks by malicious insiders are among the costliest to mitigate, at approximately USD156 per record stolen[1]—and data breaches can expose hundreds of thousands or even millions of records.

Grant access cautiously, and keep a close eye

Today's security leaders often lack the tools and the time to ensure that the principle of least privilege—restricting access based on each user's ongoing, demonstrated need—is enforced consistently. As a result, users may be granted excessive access privileges for the sake of simplicity or expediency—which can leave your organization vulnerable to attack. Tracking who needs access to what and re-certifying that access regularly becomes a large burden on the security department. As a result, it's often not done well enough, or never done at all.

Spot unauthorized use, on both sides of your firewall

Even when access starts out carefully vetted, business-critical password-protected applications are vulnerable to credential threat. However, conventional approaches to increased security can add complexity for users with additional passwords, cumbersome physical tokens, or needless interruptions. Security leaders must think of ways to protect their employees from phishing attacks, and their businesses from fraud, without disrupting their users. When a trusted user starts acting suspiciously, security solutions must spot it quickly, and react fast to revoke access.

With IBM IAM solutions, you can help secure your business by ensuring that the right people have the right access. With analytic capabilities from IBM, you'll be able to make smarter, better informed decisions about establishing or updating users' access, with the ability to uncover outliers and toxic combinations of entitlements. You'll be able to discreetly verify a user's identity when they log in and throughout their session, and to apply step-up authentication if anomalies are detected.

A recent study found that 47% of enterprise security incidents studied involved a **malicious or criminal attack**, while another 25% were rooted in negligence.[1]

▸ Learn more in this video about how IBM IAM tools can help secure your enterprise.

IBM Security IBM

1 "2017 Cost of Data Breach Study: Global overview," *Ponemon Institute,* June 2017.

Make way for business by preparing for change

Today's customers have ever-increasing expectations for their digital experiences. They demand frictionless access throughout their session, letting them focus on the product or service they're using. Taking a near-silent approach to security helps you provide this experience. One recent study highlighted that consumers who found authentication processes easy to use leverage digital services 10 to 20 percent more than customers who are frustrated by them.[1]

Step out of the user's way

Strong authentication aligned with the context of each user's access request can help deliver an unobtrusive user experience, giving enterprises a unique opportunity to differentiate themselves, and deliver value to customers and employees. Customers can seamlessly but securely purchase or interact with services and products online, and workforces—even highly mobile ones relying on a variety of devices—can collaborate with on-premises, cloud and hybrid cloud applications and tools.

Give your IT team the tools they need to foster change

The proliferation of tools and applications, both in the cloud and on-premises, places an increasing burden on IT teams to manage access requests and the security requirements of user authentication. Those teams face bottlenecks when their current tools can't keep up with the demand, application development is too slow, and user experiences do not meet expectations.

With IBM IAM you'll enable digital transformation and make way for business.

You'll be able to centralize and efficiently manage access to these tools and resources. Access management, identity lifecycle and governance can be applied consistently regardless of resource type, and your access decisions will be backed by analytics for speed and efficiency. Line-of-business managers and IT will be able to partner for better access decisions.

You'll be able to provide the experience that internal and external users have come to expect, with near-frictionless authentication, using a variety of authentication methods, without changing the applications being secured. Users will be able to leverage social-network identities for fast registration, and developers will be able to directly integrate strong authentication to deliver a seamless experience to users.

A South African financial institution using the risk-based authentication of IBM Security Access Manager saw a

99%

reduction

in fraud.[2]

Learn more about how IBM Security Access Manager can help protect your enterprise resources with risk-based access.

1 Salim Hasham, Chris Rezek, Maxence Vancauwenberghe and Josh Weiner, "Is cybersecurity incompatible with digital convenience?," *McKinsey & Company,* August 2016.

2 "Entersekt: Providing Strong Authentication and Transaction Signing Capabilities," *SecurityIntelligence.com,* January 3, 2017.

IBM Security IBM

Establish trust by knowing what's real

Businesses have long had to comply with differing regulations. From Sarbanes-Oxley (SOX) to the European Union's General Data Protection Regulation (GDPR) to the Revised Payment Services Directive (PSD2), regulations impacting IAM programs are constantly evolving. Tomorrow will bring even more national and international regulations, so businesses need to be prepared for what's next. When you can establish silent, secure IAM in your organization, you can be prepared to meet new regulations as they emerge.

Winning organizations must establish trust both internally and externally, operating with confidence that employees and customers are who they say they are through effective identity corroboration, and ensuring that departmental IAM administrators are all working from the same source of truth in terms of users and their entitlements.

Complicated data-access needs that span multi-site, multi-system environments compound the challenge of centralizing user identities and entitlements. How complicated? A recent survey of technology, financial services and professional services providers found that only 25 percent of respondents consider themselves to have well-documented records of where all data is housed[1]—but the list of needed resources just keeps growing.

Tame complicated regulated environments

IAM solutions from IBM supply powerful analytics to help you make informed decisions about identity, give users the applications and the flexible data access they need, and help to ensure compliance with compliance mandates. You can:

- Verify users' identities and that they have the legitimate access they need
- Establish trust centrally for all your applications
- Empower consumers with rights and consent through consumer identity and access management
- Implement an identity and governance solution that seamlessly integrates with even the most complex business platforms, including SAP, mainframe and midrange systems

Identity governance capabilities from IBM allow you to effectively manage access certifications and on- and off-boarding processes, and enforce the principle of least privilege. You'll have a comprehensive identity governance solution, with controls and visibility from a single application.

One multinational manufacturer used IBM identity governance solutions to manage **more than 430 million entitlements** with only a few hundred segregation-of-duties (SOD) rules.[2]

Learn how to improve access governance with intelligent entitlements.

1 Daniel Kirsch, "Prepared for the GDPR? Top 10 Findings From Hurwitz & Associates Survey," *SecurityIntelligence.com,* March 2, 2017.

2 Based on IBM customer experience.

Choose the right IBM IAM solutions for your enterprise

IAM solutions from IBM can help meet the needs of IT and security personnel, line-of-business managers, and privacy and compliance officers with unified management and governance, decision-driving analytics, and a wide range of verification methods.

IBM Security Access Manager, available as a turnkey appliance or a virtual machine image, simplifies access to resources with cross-application single sign-on, and protects enterprise assets with multi-factor authentication and risk-based access. IBM Security Access Manager also enables mobile initiatives with access control policies that help integrate mobile device management, application development and malware detection solutions. Furthermore, it helps bridge the access-control gap between on-premises and cloud environments.

IBM Security Access Manager can help mitigate insider threats by analyzing privileged access credential use across systems, applications, and platforms, providing directory service and more.

IBM Security Identity Governance and Intelligence offers a sophisticated identity governance platform that enables access governance and helps ensure regulatory compliance for IT managers and business owners. With IBM Security Identity Governance and Intelligence, you can manage all aspects of the user lifecycle, including provisioning and workflow capabilities, and integrate these capabilities with IBM Security Identity Manager and third-party tools.

IBM Security Identity Governance and Intelligence offers visibility and user access control by consolidating access entitlements and employing sophisticated algorithms for role mining, modeling and optimization.

IBM Cloud Identity offerings support users' requirements for the applications necessary for their jobs, business leaders' needs to increase productivity for a greater competitive advantage, and IT requirements to more rapidly respond to the needs of the business, all from an easy-to-implement identity-as-a-service (IDaaS) solution. Whether you are looking for a secure bridge to the cloud or a transformative makeover of your IAM environment, IBM cloud-based IAM offerings will make you a believer in the concept of uncomplicated IAM.

IBM IAM Services help you achieve early success for your IAM initiatives, working with you to architect and deploy the solutions that best match your business needs and security objectives. From strategic advisory consulting, insider threat protection, and design and deployment to managed security services, IBM security specialists offer the expertise to tackle your toughest IAM challenges.

A large state agency **reduced time demands** on administrative staff by **80%** with automated user provisioning processes using IBM Identity and Access Management solutions.[1]

▸ Watch this video to learn how you can evolve your IAM program.

1 "A large state agency reduces administrative demands by 80 percent with IBM ID Management system," *IBM Corp.,* 2015.

IBM Security

Put IBM IAM solutions into action in your enterprise

Silent security is important to your IAM solution; you should establish a plan for implementing an IAM solution that fits your employees, your business partners and your customers. You can address the pains of securing your enterprise, transforming the digital experience of your users, and keeping up with ever-changing regulatory mandates by applying the lessons of silent security for IAM throughout your information environment.

Keep your users safe, and your information secure

Protect your identities across your enterprise with seamless, analytics-backed user authentication, maximizing appropriate data access by applying step-up authentication steps as context demands.

Transform your business with IAM that gets out of the way

Provide customers, business partners and users throughout your organization a smooth digital experience by minimizing authentication procedures that interfere with seamless access and by offering your users convenient choices.

Foster privacy and trust

Protect your business by safeguarding data for regulators, auditors, and consumers, with identity and access solutions that help establish trust in every digital interaction and help you prepare for regulations that govern data sharing. Coordinate access with user-friendly interfaces that help you consolidate visibility and control over all aspects of system access.

IAM solutions from IBM combine proven technology with research-backed innovation for real-world improvements such as secure mobile access to enterprise resources and seamless logins to cloud applications such as Salesforce. Using IBM IAM, a large bank in the Nordics incorporated risk-based controls, fingerprint recognition and behavioral analysis into their single sign-on authentication across their internal systems, without having to touch the code of the applications themselves.[1] With IBM IAM, a leading credit provider in Malaysia replaced password entry processes that previously took three to five seconds with sub-second fingerprint authentication.[2]

With on-premises, IDaaS, and hybrid options, all backed by analytics and built for administrative simplicity, your enterprise, too, can help strengthen security, effect business transformation, and deepen trust—and do so across all aspects of your business.

Researchers anticipate that, for 2017, businesses will pay at least **50% more** for software as a service (SaaS) than for software licenses.[3]

Learn more about enabling digital transformation with cloud-based IBM IAM tools.

1 Based on IBM customer experience.

2 "A leading credit service provider in Asia reduces risk and increases profitability with an advanced access management solution," *IBM Security,* September 2014.

3 "SaaS Adoption 2017: If You Aren't Using SaaS Broadly, Your Business Risks Falling Behind," *Forrester Research,* June 29, 2017.

IBM Security IBM

For more information

To learn more about IAM solutions from IBM, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/identity-access-management

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
November 2017

WGW03348-USEN-00

IBM Security

IBM